UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/981,182	10/16/2001	John M. Schnizlein	50325-0560	5410

29989 7590 07/10/2007

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/981,182	SCHNIZLEIN ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-8,10,11 and 26-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-8,10,11 and 26-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 26 April 2007.

2. Claims 1, 3-8, 10, 11 and 26-38 are pending in the application.

3. Claims 1, 3-8, 10, 11 and 26-38 have been rejected.

4. Claims 2, 9 and 12-25 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 26 April 2007 has been entered.

Response to Amendment

6. The examiner approves of the amendment made to specification. No new matter has been added to the specification. The amendment overcomes the rejection. The examiner withdraws the rejection under 35 U.S.C 101.

Response to Arguments

7. Applicant's arguments with respect to claims 1, 3-8, 10, 11 and 26-38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 3, 6, 7, 9-11, 26-30, 32-35, 37 and 38 are rejected under 35 U.S.C. 102(b) as being anticipated by Sistanizadeh et al U.S. Patent No. 5,790,548.

As to claim 1, Sistanizadeh et al discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 17, lines 26-39];

receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host [column 9 line 61 to column 10 line 14];

generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data [column 12 line 31 to column 13 line 56]; and

sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host [column 12 line 31 to column 13 line 56].

wherein generating the second message further comprises the step of sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data [column 12 line 31 to column 13 line 56].

As to claims 3, 29 and 34, Sistanizadeh et al discloses a method as recited, wherein:

step of generating the second message further comprises the steps of:

storing second data based on the first data by the authenticator process [column 12 line 31 to column 13 line 56]; and

retrieving the second data by the relay agent process in response to the step of receiving the first message [column 12 line 31 to column 13 line 56].

As to claim 6, Sistanizadeh et al discloses that the physical connection comprises an Ethernet interface card on the router [column 7 line 66 to column 8 line 22].

As to claims 7, 30 and 35, Sistanizadeh et al discloses that the physical connection comprises a wireless Ethernet encryption key and time slot [column 12, lines 47-67].

As to claim 9, Sistanizadeh et al discloses that the second message is based on a dynamic host configuration protocol (DHCP) [column 11, lines 40-55].

As to claims 10, 32 and 37, Sistanizadeh et al discloses that the first data includes user class data indicating a particular group of one or more authorized users of the host [column 12 line 31 to column 13 line 56]. Sistanizadeh et al discloses that the step of generating the second message is further based on the user class data [column 12 line 31 to column 13 line 56].

As to claims 11, 33 and 38, Sistanizadeh et al discloses a method as recited, wherein:

the first data includes credential data indicating authentication is performed by the first server [column 12, lines 3-20], and

the step of generating the second message is further based on the credential data [column 12, lines 3-20].

As to claim 26, Sistanizadeh et al discloses an apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

means for receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 17, lines 26-39];

means for receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host [column 9 line 61 to column 10 line 14];

means for generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data [column 12 line 31 to column 13 line 56]; and

means for sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host [column 12 line 31 to column 13 line 56];

wherein generating the second message further comprises the step of sending a third message, from the authenticator process to the relay agent process, that contains at lest some of the authentication and authorization information based on the first data [column 12 line 31 to column 13 line 56].

As to claim 27, Sistanizadeh et al discloses an apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom [column 7 line 66 to column 8 line 22];

a physical connection that is coupled to the host [column 7 line 66 to column 8 line 22];

a processor [column 7 line 66 to column 8 line 22];

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving, at an authenticator process for the host, through the network interface from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 17, lines 26-39];

receiving, at a DHCP relay agent process, through the physical connection from the host, a DHCP discovery message for discovering a logical network address for the host [column 9 line 61 to column 10 line 14];

generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data [column 12 line 31 to column 13 line 56]; and

sending through the network interface the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host [column 12 line 31 to column 13 line 56];

wherein generating the second message further comprises the step of sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data [column 12 line 31 to column 13 line 56].

As to claim 28, Sistanizadeh et al discloses a computer-readable storage medium carrying one or more sequences of instructions for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 17, lines 26-39];

receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host [column 9 line 61 to column 10 line 14];

generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data [column 12 line 31 to column 13 line 56]; and

sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host [column 12 line 31 to column 13 line 56];

wherein generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization

information based on the first data [column 12 line 31 to column 13 line 56].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sistanizadeh et al U.S. Patent No. 5,790,548 as applied to claim 1 above, and further in view of Park US 2002/0026573 A1.

As to claims 4 and 5, Sistanizadeh et al does not teach that the first server is an authentication, authorization and accounting server. Sistanizadeh et al does not teach that that the first server is a RADIUS protocol server.

Park teaches an authentication, authorization and accounting (AAA) server that uses the RADIUS protocol [0013.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Sistanizadeh et al so that the first server sould have been an AAA server that utilized the RADIUS protocol.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Sistanizadeh et al by the teaching of Park because the RADIUS protocol message has an authenticator field for authenticating the value of the authenticator is a value that the Foreign Agent produces arbitrarily. This value is not to be

repeated; a value that has been used beforehand should not be used again. The reason why the authenticator is used as an arbitrary value is to prevent a hacker from stealing a message for malicious purposes. If the authenticator were fixed according to a message, a hacker could get a normal access-accept message from the AAA server by using the authenticator of a message produced on the basis of the commonly held secret key even though the hacker is not privy to the value of the shared secret key. Thus, the authenticator value needs to be changed every time a message is generated, thereby preventing the hacker from attacking [0013].

10. Claims 8, 31 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sistanizadeh et al U.S. Patent No. 5,790,548 as applied to claims 1, 26 and 27 above, and further in view of Bahl et al U.S. Patent No. 6,782,422 B1.

As to claims 8, 31 and 36, Sistanizadeh et al does not teach that the request for authentication is based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

Bahl et al teaches authentication based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard [column 11, lines 52-58].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Sistanizadeh et al so that the request for authentication was based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Sistanizadeh et al by the teaching of Bahl et al because that

standard of protocol is more secure connection and higher level of authentication [column 11, lines 52-58].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
July 2, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100